An Overview of Block Chain Technology and Application

Soumil Nitin Shah
Advisor Dr. Omar Abuzaghleh
Department of Electrical and Computer Engineering, University of Bridgeport, Bridgeport, CT 06604

Abstract

Cryptocurrency, and its underlying technologies, has been gaining popularity for transaction management beyond financial transactions. Transaction information is maintained in the block-chain, which can be used to audit the integrity of the transaction. The focus on this poster is the potential availability of block-chain technology of other transactional uses. Block-chain is one of the most stable open ledgers that preserves transaction information, and is difficult to forge. Since the information stored in block-chain is not related to personally identify information, it has the characteristics of anonymity. Also, the block-chain allows for transparent transaction verification since all information in the block-chain is open to the public. These characteristics are the same as the requirements for a voting system. That is, strong robustness, anonymity, and transparency. In this paper, we propose an electronic voting system as an application of block-chain, and describe block-chain based voting at a national level through examples

Introduction

The blockchain is an undeniably ingenious invention – the brainchild of a person or group of people known by the pseudonym, Satoshi Nakamoto. But since then, it has evolved into something greater, and the main question every single person is asking is: What is Blockchain? By allowing digital information to be distributed but not copied, blockchain technology created the backbone of a new type of internet. Originally devised for the digital currency, Bitcoin the tech community has now found other potential uses for the technology. Block chain is based on three main property they are as follow.

1.Decentralization

2.Transparency

3.Immutability

Decentralization Example : When you google search for something, you send a query to the server who then gets back at you with the relevant information. That is simple client-server. Now, centralized systems have treated us well for many years, however, they have several vulnerabilities example to Decentralization can be seen in Figure 1

• Firstly, because they are centralized, all the data is stored in one spot. This makes them easy target spots for potential hackers.

•If the centralized system were to go through a software upgrade, it would halt the entire system

•What if the centralized entity somehow shut down for whatever reason? That way nobody will be able to access the information that it possesses

•Worst case scenario, what if this entity gets corrupted and malicious? If that happens then all the data that is inside the blockchain will be compromised.

Transparency Example: Well… a person's identity is hidden via complex cryptography and represented only by their public address. So, if you were to look up a person's transaction history, you will not see So, while the person's real identity is secure, you will still see all the transactions that were done by their public address. This level of transparency has never existed before within a financial system. It adds that extra, and much needed, level of accountability which is required by some of these biggest institutions

Immutability Example:

Immutability, in the context of the blockchain, means that once something has been entered into the blockchain, it cannot be tampered with

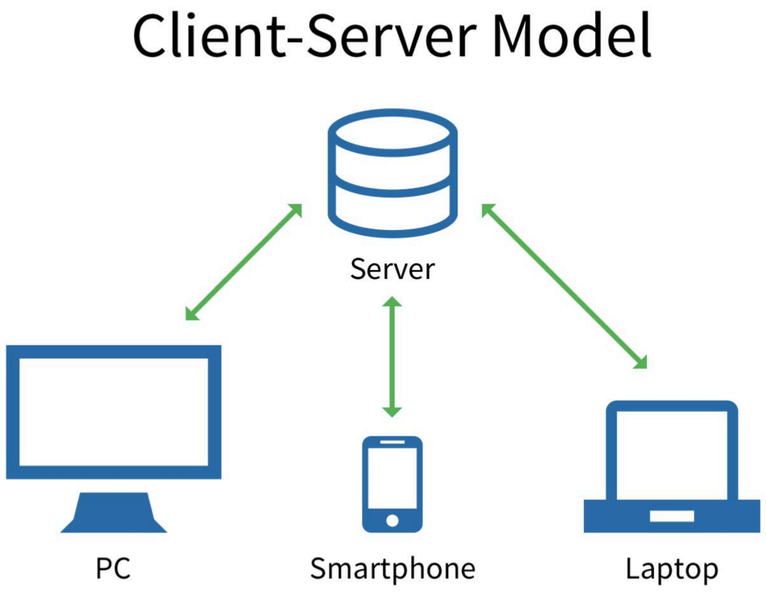

Figure 1 shows Decentralization process

Working Principle of Block Chain Technology

The block-chain is composed of time stamps which show at what time data (a block) was added. A block that contains transactions occurring at a certain time is similar to a time- stamped binary file. The hash value of the previous block and the current block will be the input of the hash value of the next block. Each hash value of a block is calculated from the hash value of the previous block, and transactions are recorded in the block. Figure 1 shows a simple Block Chain

Since The block-chain is composed of time stamps which show at what time data (a block) was added. A block that contains transactions occurring at a certain time is similar to a time- stamped binary file. The hash value of the previous block and the current block will be the input of the hash value of the next block. Each hash value of a block is calculated from the hash value of the previous block, and transactions are recorded in the block.

The block-chain is composed of time stamps which show at what time data (a block) was added. A block that contains transactions occurring at a certain time is similar to a time- stamped binary file. The hash value of the previous block and the current block will be the input of the hash value of the next block. Each hash value of a block is calculated from the hash value of the previous block, and transactions are recorded in the block.

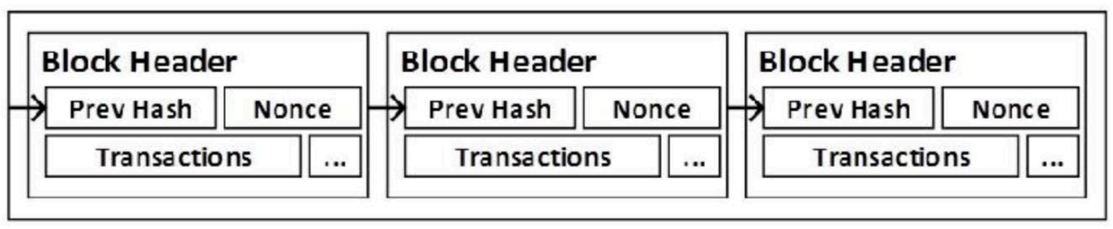

Figure 2 shows System Block Diagram

Application

Voting : Voting is an absolutely essential tool for any democratic government. It is the most important factor that makes a government.

•The paper ballot system has long been used by countries around the world. The concept is simple, you put your vote on a piece of paper and put it in a ballot box. At the end of the election, the votes are counted and whoever gets the most votes is the winner

Problem Traditional System

•The amount of time taken to count the votes is too high.

•The election can be hijacked via the insertion of bogus ballot papers.

•More powerful parties can use intimidation tactics on the venues to rig the election in a certain way.

•The amount of paper wastage can cause harm to the environment.

• There is no historical record possible to keep track of each and every vote made.

•The cost of expenditure on paper ballots is very high.

•It is impossible to keep track of your vote.

•Once you have cast a vote you cannot change it.

Problem Digital System

•So as you can see, there are a lot of disadvantages of a paper ballot system. To counter this a digital voting system has several disadvantage

•Firstly, the client side machine could develop a malware which reads each and every vote cast and changes the vote to the other candidate.

•An attacker can directly infect the servers through malware placed on the DVDs used to set up the servers and transfer the votes

Conclusion

So as you can see, there are a lot of disadvantages of a paper ballot system. To counter this a digital voting system has several disadvantage Firstly, the client side machine could develop a malware which reads each and every vote cast and changes the vote to the other candidate. An attacker can directly infect the servers through malware placed on the DVDs used to set up the servers and transfer the votes the solution to above mentioned probel is Block chain